

1 CLAIM AMENDMENTS

2 Listing of Claims:

3 What is claimed, is

4 CLAIMS

5 1. (original) A method for providing a user device with a set of
6 access codes, the method comprising:

7 in the user device, storing an encryption key and an
8 identification code, and sending a message containing the
9 identification code to a server via a communications network;

10 in the server, storing an encryption key corresponding to
11 the key stored in the user device, allocating the set of access
12 codes on receipt of the identification code from the user device,
13 performing a look up function based on the identification code
14 received in the message to retrieve the key from storage,
15 encrypting the set of access codes using the retrieved key to
16 produce an encrypted set, and sending a message containing the
17 encrypted set to the user device via the network; and,

18 in the user device, decrypting the encrypted set received
19 from the server using the key in storage, and storing the
20 decrypted set of access codes for use by a user of the user
21 device; and,

22 upon the number of unused access codes reaching a
23 predetermined threshold, in the server, sending a message
24 containing a new set of access codes to the user device via the
25 network; and,

26 in the user device, storing the new set for use by a user of
27 the user device.

28 2. (original) A method as claimed in claim 1, further comprising:

1 in the user device, tracking the access codes used by the
2 user, generating a request in response to the number of unused
3 access codes reaching a predetermined threshold, and sending a
4 message containing the request to the server; and,
5 in the server, sending the message containing the new set of
6 access codes on receipt of the request.

7 3. (original) A method as claimed in claim 1, further comprising:
8 in the server, tracking the access codes used by the user, and
9 sending the message containing the new set of access codes to the
10 user device in response to the number of unused access codes
11 reaching a predetermined threshold.

12 4. (original) A method as claimed in claim 1, further comprising:
13 in the server, generating a new key, encrypting the new key
14 with the previous key, and sending a message containing the
15 encrypted new key to the user device via the network; and, in the
16 user device, decrypting the new key received from the server
17 using the previous key, and storing the decrypted new key in
18 place of the previous key.

19 5. (original) A method as claimed in claim 4, further comprising:
20 in the server, encrypting a new set of access codes with the
21 new key to produce a new key encrypted set, and sending a message
22 containing the new key encrypted set to the user device via the
23 network; and,
24 in the user device, decrypting the new key encrypted set
25 using the new key, and storing the decrypted new set for use by a
26 user of the user device.

27 6. (original) A method as claimed in claim 1, further comprising:
28 in the user device, generating a public/private key pair,
29 and sending a message containing the public key of the pair to
30 the server via the network;

1 in the server, generating a session key, encrypting the set
2 of access codes with the session key to produce a session key
3 encrypted set, encrypting the session key with the public key to
4 produce an encrypted session key, sending a message containing
5 the session key encrypted set and the encrypted session key to
6 the user device via the network; and,

7 in the user device, decrypting the encrypted session key
8 with the private key of the pair to recover the session key,
9 decrypting the session key encrypted set with the recovered
10 session key to recover the set, and storing the decrypted set for
11 use by a user of the user device.

12 7. (original) A method for providing a user device with a set of
13 access codes, the method comprising, in the user device:

14 storing an encryption key and an identification code;

15 sending a message containing the identification code to a
16 server via a communications network;

17 receiving from the server a message containing the set of
18 access codes encrypted with the key;

19 decrypting the received set of access codes using the key in
20 storage; and,

21 storing the decrypted set of access codes for use by a user
22 of the user device.

23 upon the number of unused access codes reaching a
24 predetermined threshold, receiving from the server a message
25 containing a new set of access codes; and,

26 in the user device, storing the new set for use by a user of
27 the user device.

28 8. (original) A method as claimed in claim 7, further comprising:
29 in the user device, tracking the access codes used by the user,
30 generating a request in response to the number of unused access
31 codes reaching a predetermined threshold, and sending a message
32 containing the request to the server.

1 9. (original) A method as claimed in claim 7, further comprising,
2 in the user device:

3 decrypting a new key received from the server using the
4 previous key; and,
5 storing the decrypted new key in place of the previous key.

6 10. (original) A method as claimed in claim 9, further
7 comprising, in the user device:

8 receiving from the server a message containing a new key
9 encrypted set of access codes via the network;
10 decrypting the new key encrypted set using the new key; and,
11 storing the decrypted new set for use by a user of the user
12 device.

13 11. (original) A method as claimed in claim 7, comprising, in the
14 user device:

15 generating a public/private key pair;
16 sending a message containing the public key of the pair to
17 the server via the network;
18 receiving a message containing a session key encrypted set
19 of access codes and a public key encrypted session key from the
20 server via the network;
21 decrypting the public key encrypted session key with the
22 private key of the pair to recover a session key encrypted set
23 and a corresponding session key;
24 decrypting the session key encrypted set with the recovered
25 session key to recover the set; and,
26 storing the decrypted set for use by a user of the user
27 device.

28 12. (currently amended) A computer program element comprising
29 computer program code mean when loaded in a processor of a user
30 device, configures the processor to perform a method as claimed
31 in ~~any of claims~~ claim 7 to 11.

1 13. (original) A method for providing a user device with a set of
2 access codes, the method comprising, in a server for
3 communicating with the user device via a network:

4 storing an encryption key corresponding to an encryption key
5 stored in the user device;

6 allocating the set of access codes to the user device on
7 receipt of a message containing an identification code from the
8 user device via the network;

9 performing a look up function based on the identification
10 code received in the message to retrieve the key from storage;

11 encrypting the set of access codes using the retrieved key
12 to produce an encrypted set; and,

13 sending a message containing the encrypted set to the user
14 device via the network; and,

15 upon the number of unused access codes reaching a
16 predetermined threshold, sending a message containing a new set
17 of access codes to the user device via the network.

18 14. (currently amended) A method as claimed in claim 13, further
19 comprising, in the server:

20 generating a new key, encrypting the new key with the
21 previous key; and,

22 sending a message containing the encrypted new key to the
23 user device via the network. ~~and,~~

24 15. (original) A method as claimed in claim 14, further
25 comprising, in the server:

26 encrypting the new set of access codes with the new key to
27 produce a new key encrypted set of access codes.

28 16. (original) A method as claimed in claim 13, further
29 comprising, in the server:

30 receiving a message containing a public key of a
31 public/private key pair from the user device;

32 generating a session key;

1 encrypting the set of access codes with the session key to
2 produce a session key encrypted set;
3 encrypting the session key with the public key to produce a
4 public key encrypted session key; and,
5 sending a message containing the session key encrypted set
6 and the public key encrypted session key to the user device via
7 the network.

8 17. (currently amended) A computer program element comprising
9 computer program code means when loaded in a processor of a
10 server computer system, configures the processor to perform a
11 method as claimed in ~~any of claims~~ claim 13 to 16.

12 18. (currently amended) A method as claimed in ~~any of claims~~
13 claim 1 to 16, further comprising a limitation taken from a group
14 of limitations consisting of:

15 wherein the access codes are one time authentication codes;

16 wherein the network comprises a wireless communication
17 network;

18 wherein the user device comprises one of a mobile phone, a
19 personal digital assistant, and a smart card; and

20 wherein the messages are SMS messages.

21 19-21 (canceled)

22 22. (currently amended) An apparatus for providing a user with a
23 set of access codes, the apparatus comprising: a user device;
24 and, server for communicating with the user device via a
25 communications network; the user device comprising
26 means for storing an encryption key and an identification
27 code, and

1 means for sending a message containing the identification
2 code to the server via the network; the server comprising
3 means for storing an encryption key corresponding to the key
4 stored in the user device,
5 means for allocating the set of access codes on receipt of
6 the identification code from the user device,
7 means for performing a look up function based on the
8 identification code received in the message to retrieve the key
9 from storage,
10 means for encrypting the set of access codes using the
11 retrieved key to produce an encrypted set, and
12 means for sending a message containing the encrypted set to
13 the user device via the network and for sending upon the number
14 of unused access codes reaching a predetermined threshold, a
15 message containing a new set of access codes to the user device
16 via the network; and, in the user device, storing the new set for
17 use by a user of the user device.
18 and, the user device further comprising:
19 means for decrypting the encrypted set received from the
20 server using the key stored in the user device, and
21 means for storing the decrypted set of access codes for use
22 by the user.

23 23. (original) Apparatus as claimed in claim 22, wherein the
24 server further comprises

25 means for generating a new key,
26 means for encrypting the new key with the previous key, and
27 means for sending a message containing the encrypted new key
28 to the user device via the network, and wherein the user device
29 further comprises
30 means for decrypting the new key received from the server
31 using the previous key, and
32 means for storing the decrypted new key in place of the
33 previous key.

1 24. (original) Apparatus as claimed in claim 23, wherein the
2 server further comprises
3 means for encrypting the new set of access codes with the
4 new key to produce a new key encrypted set; and
5 means for sending a message containing the new key encrypted
6 set to the user device via the network, and wherein the user
7 device further comprises
8 means for decrypting the new key encrypted set using the new
9 key, and
10 means for storing the decrypted new set for use by a user of
11 the user device.

12 25. (original) Apparatus as claimed in claim 22, further
13 comprising at least one element taken from a group of elements
14 consisting of,

15 in the user device;

16 means for storing the new set for use by a user of the user
17 device;-

18 means for tracking the access codes used by the user,

19 means for generating a request in response to the number of
20 unused access codes reaching a predetermined threshold, and

21 means for sending a message containing the request to the
22 server; and

23 means for generating a request in response to a manual input
24 from the user, and

25 means for sending a message containing the request to the
26 server; and

27 in the server,

28 means for sending the message containing the new set of
29 access codes on receipt of the request; and

1 means for sending the message containing the new set of
2 access codes on receipt of the request.

3 26. (canceled)

4 27. (original) Apparatus as claimed in claim 25, further
5 comprising: in the server,
6 means for tracking the access codes used by the user, and
7 means for sending the message containing the new set of
8 access codes to the user device in response to the number of
9 unused access codes reaching a predetermined threshold.

10 28. (original) Apparatus as claimed in claim 25, further
11 comprising: in the user device,
12 means for generating a request in response to a manual input
13 from the user, and
14 means for sending a message containing the request to the
15 server; and, in the server,
16 means for sending the message containing the new set of
17 access codes on receipt of the request.

18 29. (original) Apparatus as claimed in claim 22, wherein the user
19 device further comprises
20 means for generating a public/private key pair and
21 means for sending a message containing the public key of the
22 pair to the server via the network; wherein the server further
23 comprises
24 means for generating a session key,
25 means for encrypting the set of access codes with the
26 session key to produce a session key encrypted set,
27 means for encrypting the session key with the public key to
28 produce a public key encrypted session key, and
29 means for sending a message containing the session key
30 encrypted set and the public key encrypted session key to the

1 user device via the network; and, wherein the user device further
2 comprises

3 means for decrypting the public key encrypted session key
4 with the private key of the pair to recover the session key,

5 means for decrypting the session key encrypted set with the
6 recovered session key to recover the set, and

7 means for storing the decrypted set for use by a user of the
8 user device.

9 30. (currently amended) An apparatus as claimed in any of claims
10 claim 22 to 29, further comprising a limitation taken from a
11 group of limitations consisting of:

12 wherein the access codes are one time authentication codes;

13 ~~wherein the network comprises a wireless communication~~
14 ~~network;~~

15 ~~wherein the user device comprises one of a mobile phone, a~~
16 ~~personal digital assistant, and a smart card; and~~

17 ~~wherein the messages are SMS messages.~~

18 31-33 (canceled)

19 34. (original) A user device for receiving a set of access codes
20 from a server via a communications network, the device
21 comprising:

22 means for storing an encryption key and an identification
23 code;

24 means for sending a message containing the identification
25 code to a server via a communications network;

26 means for receiving from the server a message containing the
27 set of access codes encrypted with the key;

1 means for decrypting the received set of access codes using
2 the key in storage; and,
3 means for storing the decrypted set of access codes for use
4 by a user of the user device; and
5 means for receiving upon the number of unused access codes
6 reaching a predetermined threshold from the server a message
7 containing a new key encrypted set of access codes via the
8 network.

9 35. (original) A user device as claimed in claim 34, further
10 comprising:

11 means for decrypting a new key received from the server
12 using the previous key; and,

13 means for storing the decrypted new key in place of the
14 previous key.

15 36. (original) A user device as claimed in claim 35, further
16 comprising:

17 means for decrypting the new key encrypted set using the new key;
18 and,

19 means for storing the decrypted new set for use by a user of the
20 user device.

21 37. (original) A user device as claimed in claim 34, further
22 comprising:

23 means for generating a public/private key pair;

24 means for sending a message containing the public key of the
25 pair to the server via the network;

26 means for receiving a message containing a session key
27 encrypted set of access codes and a public key encrypted session
28 key from the server via the network;

29 means for decrypting the public key encrypted session key
30 with the private key of the pair to recover the session key;

31 means for decrypting the session key encrypted set with the
32 recovered session key to recover the set; and,

1 means for storing the decrypted set for use by a user of the
2 user device.

3 38. (original) A server for providing a user device with a set of
4 access codes via a communications network, the server comprising:

5 means for storing an encryption key corresponding to an
6 encryption key stored in the user device;

7 means for allocating the set of access codes to the user
8 device on receipt of a message containing an identification code
9 from the user device via the network;

10 means for performing a look up function based on the
11 identification code received in the message to retrieve the key
12 from storage;

13 means for encrypting the set of access codes using the
14 retrieved key to produce an encrypted set; and,

15 means for sending a message containing the encrypted set to
16 the user device via the network,

17 means for sending upon the number of unused access codes
18 reaching a predetermined threshold a message containing the new
19 set of access codes to the user device via the network.

20 39. (original) A server as claimed in claim 38, further
21 comprising at least one element taken from a group of elements
22 consisting of:

23 means for generating a new key, encrypting the new key with
24 the previous key, ~~and~~

25 means for sending a message containing the encrypted new key
26 to the user device via the network; ~~and~~

27 means for encrypting the new set of access codes with the
28 new key to produce a new key encrypted set;

29 means for receiving a message containing a public key of a
30 public/private key pair from the user device,

1 means for generating a session key,
2 means for encrypting the set of access codes with the
3 session key to produce a session key encrypted set,
4 means for encrypting the session key with the public key to
5 produce a public key encrypted session key, and
6 means for sending a message containing the session key
7 encrypted set and the public key encrypted session key to the
8 user device via the network.

9 40-41. (canceled)

10